

Defining \mathbb{Z} in \mathbb{Q}

Jochen Koenigsmann

20/10/2010

Abstract

We show that \mathbb{Z} is definable in \mathbb{Q} by a universal first-order formula in the language of rings. We also present an $\forall\exists$ -formula for \mathbb{Z} in \mathbb{Q} with just one universal quantifier. We exhibit new diophantine subsets of \mathbb{Q} like the set of non-squares or the complement of the image of the norm map under a quadratic extension. Finally, we show that there is no existential formula for \mathbb{Z} in \mathbb{Q} , provided one assumes a strong variant of the Bombieri-Lang Conjecture for varieties over \mathbb{Q} with many \mathbb{Q} -rational points.¹

1 \mathbb{Z} is universally definable in \mathbb{Q}

Hilbert's 10th problem was to find a general algorithm for deciding, given any n and any polynomial $f \in \mathbb{Z}[x_1, \dots, x_n]$, whether or not f has a zero in \mathbb{Z}^n . Building on earlier work by Martin Davis, Hilary Putnam and Julia Robinson, Yuri Matiyasevich proved in 1970 that there can be no such algorithm. In particular, the existential first-order theory $\text{Th}_{\exists}(\mathbb{Z})$ of \mathbb{Z} (in the language of rings $\mathcal{L} := \{+, \cdot, 0, 1\}$) is undecidable. Hilbert's 10th problem over \mathbb{Q} , i.e. the question whether $\text{Th}_{\exists}(\mathbb{Q})$ is decidable, is still open.

If one had an **existential** (or **diophantine**) definition of \mathbb{Z} in \mathbb{Q} (i.e. a definition by an existential 1st-order \mathcal{L} -formula), then $\text{Th}_{\exists}(\mathbb{Z})$ would be interpretable in $\text{Th}_{\exists}(\mathbb{Q})$, and the answer would, by Matiyasevich's Theorem, again be no. But it is still open whether \mathbb{Z} is existentially definable in \mathbb{Q} , and, in fact, towards the end of the paper we provide strong reasons why it shouldn't (Theorem 20).

¹2000 *Mathematics Subject Classification*. Primary 11U05; Secondary 11R52, 11G35, 11U09.

Key words and phrases. Hilbert's Tenth Problem, diophantine set, undecidability, definability, quaternion algebra, Bombieri-Lang Conjecture.

The research on this paper started while the author enjoyed the hospitality of the Max-Planck-Institut Bonn.

The earliest 1st-order definition of \mathbb{Z} in \mathbb{Q} , due to Julia Robinson ([R]) can be expressed by an $\forall\exists\forall$ -formula of the shape

$$\phi(t) : \forall x_1 \forall x_2 \exists y_1 \dots \exists y_7 \forall z_1 \dots \forall z_6 f(t; x_1, x_2; y_1, \dots, y_7; z_1, \dots, z_6) = 0$$

for some $f \in \mathbb{Z}[t; x_1, x_2; y_1, \dots, y_7; z_1, \dots, z_6]$, i.e. for any $t \in \mathbb{Q}$,

$$t \in \mathbb{Z} \text{ iff } \phi(t) \text{ holds in } \mathbb{Q}.$$

Recently, Bjorn Poonen ([P1]) managed to find an $\forall\exists$ -definition with 2 universal and 7 existential quantifiers. In this paper we present an \forall -definition of \mathbb{Z} in \mathbb{Q} . To look out for such a creature may well be excused by, and, indeed, was founded on, the following rather basic

Observation 0 *If there is an existential definition of \mathbb{Z} in \mathbb{Q} then there is also a universal one.*

Proof: If \mathbb{Z} is diophantine in \mathbb{Q} then so is

$$\mathbb{Q} \setminus \mathbb{Z} = \{x \in \mathbb{Q} \mid \exists m, n, a, b \in \mathbb{Z} \text{ with } m \neq 0, n \neq 0, \pm 1, am + bn = 1 \text{ and } m = xn\}.$$

□

Theorem 1. *There is a polynomial $g \in \mathbb{Z}[t; x_1, \dots, x_{418}]$ of degree 28 such that, for any $t \in \mathbb{Q}$,*

$$t \in \mathbb{Z} \text{ iff } \forall x_1 \dots \forall x_{418} \in \mathbb{Q} \ g(t; x_1, \dots, x_{418}) \neq 0.$$

If one measures logical complexity in terms of the number of changes of quantifiers then this is the simplest definition of \mathbb{Z} in \mathbb{Q} , and, in fact, it is the simplest possible: there is no quantifier-free definition of \mathbb{Z} in \mathbb{Q} .

Corollary 2. *$\mathbb{Q} \setminus \mathbb{Z}$ is diophantine in \mathbb{Q} .*

In more geometric terms, this says

Corollary 2' *There is a (not necessarily irreducible) affine variety V over \mathbb{Q} and a \mathbb{Q} -morphism $\pi : V \rightarrow \mathbb{A}^1$ such that the image of $V(\mathbb{Q})$ is $\mathbb{Q} \setminus \mathbb{Z}$.*

Together with the undecidability of $\text{Th}_{\exists}(\mathbb{Z})$, Theorem 1 immediately implies

Corollary 3. *$\text{Th}_{\forall\exists}(\mathbb{Q})$ is undecidable.*

This was proved conditionally, using a conjecture on elliptic curves, in [CZ]. Again, we can phrase this in more geometric terms:

Corollary 3' *There is no algorithm that decides on input a \mathbb{Q} -morphism $\pi :$*

$V \rightarrow W$ between affine \mathbb{Q} -varieties V, W whether or not $\pi : V(\mathbb{Q}) \rightarrow W(\mathbb{Q})$ is surjective.

Acknowledgement: Among many others, I would, in particular, like to thank Boris Zilber, Jonathan Pila, Marc Hindry and Joseph Silverman for most helpful discussions.

2 The proof of Theorem 1

Like all previous definitions of \mathbb{Z} in \mathbb{Q} , we use local class field theory and Hasse's Local-Global-Principle for quadratic forms. What is new in our approach is the use of the Quadratic Reciprocity Law (in Proposition 13) and, inspired by the model theory of local fields, the transformation of some existential formulas into universal formulas (Step 4). A technical key trick is the existential definition of the Jacobson radical of certain rings (Step 3) which makes implicit use of so-called 'rigid elements' as they occur e.g. in [K].

Step 1: Diophantine definition of quaternionic semi-local rings à la Poonen

The first step modifies Poonen's proof ([P1]), thus arriving at a formula for \mathbb{Z} in \mathbb{Q} which, like the formula in his Theorem 4.1, has 2 \forall 's followed by 7 \exists 's, but we managed to bring down the degree of the polynomial involved from 9244 to 8.

Definition 4. For $a, b \in \mathbb{Q}^\times$, let

- $H_{a,b} := \mathbb{Q} \cdot 1 \oplus \mathbb{Q} \cdot \alpha \oplus \mathbb{Q} \cdot \beta \oplus \mathbb{Q} \cdot \alpha\beta$ be the quaternion algebra over \mathbb{Q} with multiplication defined by $\alpha^2 = a$, $\beta^2 = b$ and $\alpha\beta = -\beta\alpha$,
- $\Delta_{a,b} := \{p \in \mathbb{P} \cup \{\infty\} \mid H_{a,b} \otimes \mathbb{Q}_p \not\cong M_2(\mathbb{Q}_p)\}$ the set of primes (including ∞) where $H_{a,b}$ does not split locally ($\mathbb{Q}_\infty := \mathbb{R}$ and \mathbb{P} denotes the set of rational primes) — $\Delta_{a,b}$ is always finite, and $\Delta_{a,b} = \emptyset$ iff $a \in N(b)$, i.e. a is in the image of the norm map $\mathbb{Q}(\sqrt{b}) \rightarrow \mathbb{Q}$,
- $S_{a,b} := \{2x_1 \in \mathbb{Q} \mid \exists x_2, x_3, x_4 \in \mathbb{Q} : x_1^2 - ax_2^2 - bx_3^2 + abx_4^2 = 1\}$ the set of traces of norm-1 elements of $H_{a,b}$, and
- $T_{a,b} := S_{a,b} + S_{a,b}$ — note that $T_{a,b}$ is an existentially defined subset of \mathbb{Q} . Here we deviate from Poonen's terminology: his $T_{a,b}$ is $S_{a,b} + S_{a,b} + \{0, 1, \dots, 2309\}$.

An explicit criterion for checking whether or not an element $p \in \mathbb{P} \cup \{\infty\}$ belongs to $\Delta_{a,b}$, is given in the following

Observation 5. Assume $a, b \in \mathbb{Q}^\times$ and $p \in \mathbb{P} \cup \{\infty\}$. Then $p \in \Delta_{a,b}$ iff

for $p = 2$: After multiplying by suitable rational squares and integers $\equiv 1 \pmod{8}$ and, possibly, swapping a and b , the pair (a, b) is one of the following:

$$\begin{array}{ccccc} (2, 3) & (3, 3) & (5, 6) & (6, 6) & (15, 15) \\ (2, 5) & (3, 10) & (5, 10) & (6, 15) & (15, 30) \\ (2, 6) & (3, 15) & (5, 30) & (10, 30) & (30, 30) \\ (2, 10) & & & & \end{array}$$

for $2 \neq p \in \mathbb{P}$:

$$\begin{aligned} &v_p(a) \text{ is odd, } v_p(b) \text{ is even, and } \left(\left(\frac{b}{p}\right)\right) = -1, \text{ or} \\ &v_p(a) \text{ is even, } v_p(b) \text{ is odd, and } \left(\left(\frac{a}{p}\right)\right) = -1, \text{ or} \\ &v_p(a) \text{ is odd, } v_p(b) \text{ is odd, and } \left(\left(\frac{-ab}{p}\right)\right) = -1, \end{aligned}$$

where we use the **generalized Legendre symbol** $\left(\left(\frac{a}{p}\right)\right) = \pm 1$ to indicate whether or not the p -adic unit $ap^{-v_p(a)}$ is a square modulo p (v_p denotes the p -adic valuation on \mathbb{Q}).

for $p = \infty$: $a < 0$ and $b < 0$.

Proposition 6. For any $a, b \in \mathbb{Q}^\times$,

$$T_{a,b} = \bigcap_{p \in \Delta_{a,b}} \mathbb{Z}_{(p)},$$

where $\mathbb{Z}_{(\infty)} := \{x \in \mathbb{Q} \mid -4 \leq x \leq 4\}$, and where $T_{a,b} = \mathbb{Q}$ if $\Delta_{a,b} = \emptyset$.

Proof: For each $p \in \mathbb{P}$, let

$$U_p := \{s \in \mathbb{F}_p \mid x^2 - sx + 1 \text{ is irreducible over } \mathbb{F}_p\}$$

and let $\phi_p : \mathbb{Z}_p \rightarrow \mathbb{F}_p$ denote the p -adic place. We shall use the following

Facts For any $a, b \in \mathbb{Q}^\times$ and for any $p \in \mathbb{P}$:

- (a) If $p \notin \Delta_{a,b}$ then $S_{a,b}(\mathbb{Q}_p) = \mathbb{Q}_p$.
- (b) If $p \in \Delta_{a,b}$ then $\phi_p^{-1}(U_p) \subseteq S_{a,b}(\mathbb{Q}_p) \subseteq \mathbb{Z}_p$.
- (c) $S_{a,b}(\mathbb{R}) = \begin{cases} \mathbb{R} & \text{for } a > 0 \text{ or } b > 0 \\ [-2, 2] & \text{for } a, b < 0 \end{cases}$
- (d) If $p > 11$ then $\mathbb{F}_p = U_p + U_p$.
- (e) $S_{a,b}(\mathbb{Q}) = \mathbb{Q} \cap \bigcap_{p \in \Delta_{a,b}} S_{a,b}(\mathbb{Q}_p)$.

(a) and (b) are [P1], Lemma 2.1, (c) is a straightforward computation, (d) is [P1], Lemma 2.3, and (e) is a special case of the Hasse-Minkowski local-global principle for representing rationals by quadratic forms.

(b) and (c) immediately give the inclusion $T_{a,b} \subseteq \bigcap_{p \in \Delta_{a,b}} \mathbb{Z}_{(p)}$.

To prove the converse inclusion $T_{a,b} \supseteq \bigcap_{p \in \Delta_{a,b}} \mathbb{Z}_{(p)}$, let us first compute U_p for the primes $p \leq 11$:

$$\begin{aligned} U_2 &= \{1\} \\ U_3 &= \{0\} \\ U_5 &= \{1, 4\} \\ U_7 &= \{0, 3, 4\} \\ U_{11} &= \{0, 1, 5, 6, 10\} \end{aligned}$$

For each $p \in \mathbb{P} \cup \{\infty\}$ define $V_p \subseteq \mathbb{Z}_p$ as follows:

$$V_p = \begin{cases} \phi_2^{-1}(U_2) \cup (4 + 8\mathbb{Z}_2) & \text{for } p = 2 \\ \phi_p^{-1}(U_p) \cup [(\pm 2 + p\mathbb{Z}_p) \setminus (\pm 2 + p^2\mathbb{Z}_p)] & \text{for } 3 \leq p \leq 11 \\ \phi_p^{-1}(U_p) & \text{for } 11 < p \in \mathbb{P} \\ [-2, 2] & \text{for } p = \infty \end{cases}$$

(We define \mathbb{Z}_∞ to be the real interval $[-4, 4] \subseteq \mathbb{R}$.)

By Fact (b), Fact (c), Observation 5 together with an easy direct calculation in the cases $p = 3, 5, 7, 11$ and, for $p = 2$, by the second table in the appendix, one always has

$$V_p \subseteq S_{a,b}(\mathbb{Q}_p) \text{ and, for } p \neq \infty, V_p \text{ is open.}$$

Fact (d) and another elementary case-by-case-check for $p \leq 11$ shows that for any $p \in \mathbb{P} \cup \{\infty\}$

$$\mathbb{Z}_p = V_p + V_p.$$

Now pick $t \in \bigcap_{p \in \Delta_{a,b}} \mathbb{Z}_{(p)}$. For each $p \in \Delta_{a,b}$, there is some $s_p \in \mathbb{Z}_p$ such that $s_p, t - s_p \in V_p$.

If $t = \pm 4$ then, clearly, $t = \pm 2 \pm 2 \in S_{a,b} + S_{a,b} = T_{a,b}$.

If $t \neq \pm 4$ and $\infty \in \Delta_{a,b}$ we can choose $s_\infty \in \mathbb{Z}_\infty = \mathbb{R}$ such that $s_\infty, t - s_\infty \in]-2, 2[$. Now approximate the finitely many $s_p \in \mathbb{Z}_p$ ($p \in \Delta_{a,b}$) by a single $s \in \mathbb{Q}$ such that

$$s - s_p \in \begin{cases} 8\mathbb{Z}_2 & \text{if } p = 2 \\ p^2\mathbb{Z}_p & \text{if } 3 \leq p \leq 11 \\ p\mathbb{Z}_p & \text{if } 11 < p \in \mathbb{P} \\]-\epsilon, \epsilon[& \text{if } p = \infty \end{cases}$$

where $\epsilon = \min\{|2 \pm s_\infty|, |2 \pm (t - s_\infty)|\}$. This guarantees that for all $p \in \Delta_{a,b}$

$$s, t - s \in V_p \subseteq S_{a,b}(\mathbb{Q}_p),$$

and hence, by Fact **(e)**, that $s, t - s \in S_{a,b} = S_{a,b}(\mathbb{Q})$. \square

One then obtains an $\forall\exists$ -definition of \mathbb{Z} in \mathbb{Q} from the fact that

$$\mathbb{Z} = \bigcap_{l \in \mathbb{P}} \mathbb{Z}_{(l)} = \bigcap_{a,b > 0} T_{a,b}$$

as in [P1], Theorem 4.1. With our simplified $T_{a,b}$, the formula now becomes, for any $t \in \mathbb{Q}$,

$$\begin{aligned} t \in \mathbb{Z} \iff & \forall a, b \exists x_1, x_2, x_3, x_4, y_2, y_3, y_4 \\ & (a + x_1^2 + x_2^2 + x_3^2 + x_4^2) \cdot (b + x_1^2 + x_2^2 + x_3^2 + x_4^2) \cdot \\ & [(x_1^2 - ax_2^2 - bx_3^2 + abx_4^2 - 1)^2 + \\ & + ((t - 2x_1)^2 - 4ay_2^2 - 4by_3^2 + 4aby_4^2 - 4)^2] = 0 \end{aligned}$$

Step 2: Towards a uniform diophantine definition of all $\mathbb{Z}_{(p)}$'s in \mathbb{Q}

We will present a diophantine definition for the local rings $\mathbb{Z}_{(p)} = \mathbb{Z}_p \cap \mathbb{Q}$ depending on the congruence of the prime p modulo 8, and involving p (and if $p \equiv 1 \pmod{8}$ an auxiliary prime q) as a parameter. However, since in any first-order definition of a subset of \mathbb{Q} we can only quantify over the elements of \mathbb{Q} , and not, e.g., over all primes, we will allow arbitrary (non-zero) rationals p and q as parameters in the following definition.

Definition 7. For $p, q \in \mathbb{Q}^\times$, let

- $R_p^{[3]} := T_{-p, -p} + T_{2p, -p}$
- $R_p^{[5]} := T_{-2p, -p} + T_{2p, -p}$

- $R_p^{[7]} := T_{-p,-p} + T_{2p,p}$
- $R_{p,q}^{[1]} := T_{2pq,q} + T_{-2pq,q}$

The R 's are existentially defined subrings of \mathbb{Q} containing \mathbb{Z} since, for any $a, b, c, d \in \mathbb{Q}^\times$,

$$T_{a,b} + T_{c,d} = \bigcap_{l \in \Delta_{a,b} \cap \Delta_{c,d}} \mathbb{Z}_{(l)},$$

and since in each case at least one of a, b, c, d is > 0 , so $\infty \notin \Delta_{a,b} \cap \Delta_{c,d}$.

Explicit formulas: For $p \in \mathbb{Q}^\times$, we define

$$\begin{aligned} f_p^{[3]} := & (x_1^2 + px_2^2 + px_3^2 + p^2x_4^2 - 1)^2 + (x_5^2 + px_6^2 + px_7^2 + p^2x_8^2 - 1)^2 \\ & + (x_9^2 - 2px_{10}^2 + px_{11}^2 - 2p^2x_{12}^2 - 1)^2 \\ & + ((t - 2x_1 - 2x_5 - 2x_9)^2 - 8px_{13}^2 + 4px_{14}^2 - 8p^2x_{15}^2 - 4)^2 \end{aligned}$$

Then $f_p^{[3]}$ is a polynomial of degree 4 with parameter p such that, for any $t \in \mathbb{Q}$,

$$t \in R_p^{[3]} \iff \exists x_1, \dots, x_{15} \ f_p^{[3]}(t; x_1, \dots, x_{15}) = 0.$$

It is clear how to find very similar polynomials $f_p^{[5]}$, $f_p^{[7]}$ and $f_{p,q}^{[1]}$.

Definition 8. (a) $\mathbb{P}^{[k]} := \{l \in \mathbb{P} \mid l \equiv k \pmod{8}\}$, where $k = 1, 3, 5$ or 7

(b) For $p \in \mathbb{Q}^\times$, define

- $\mathbb{P}(p) := \{l \in \mathbb{P} \mid v_l(p) \text{ is odd}\}$
- $\mathbb{P}^{[k]}(p) := \mathbb{P}(p) \cap \mathbb{P}^{[k]}$, where $k = 1, 3, 5$ or 7
- $p \equiv_2 k \pmod{8}$ iff $p \in k + 8\mathbb{Z}_{(2)}$, where $k \in \{0, 1, 2, \dots, 7\}$.

Proposition 9. (a) $\mathbb{Z}_{(2)} = T_{3,3} + T_{2,5}$

(b) For $p \in \mathbb{Q}^\times$ and $k = 3, 5$ or 7 ,

$$R_p^{[k]} = \begin{cases} \bigcap_{l \in \mathbb{P}^{[k]}(p)} \mathbb{Z}_{(l)} & \text{if } p \equiv_2 k \pmod{8} \\ \bigcap_{l \in \mathbb{P}^{[k]}(p)} \mathbb{Z}_{(l)} \text{ or } \bigcap_{l \in \mathbb{P}^{[k]}(p) \cup \{2\}} \mathbb{Z}_{(l)} & \text{otherwise} \end{cases}$$

(As before, $\bigcap_{l \in \emptyset} \mathbb{Z}_{(l)} = \mathbb{Q}$.)

In particular, if p is a prime ($\equiv k \pmod{8}$) then $\mathbb{Z}_{(p)} = R_p^{[k]}$.

(c) For $p, q \in \mathbb{Q}^\times$ with $p \equiv_2 1 \pmod{8}$ and $q \equiv_2 3 \pmod{8}$,

$$R_{p,q}^{[1]} = \begin{cases} \bigcap_{l \in \mathbb{P}(p,q)} \mathbb{Z}_{(l)} & \text{if } \mathbb{P}(p,q) \neq \emptyset \\ \mathbb{Q} & \text{if } \mathbb{P}(p,q) = \emptyset \end{cases}$$

where

$$l \in \mathbb{P}(p, q) :\Leftrightarrow l \in \begin{cases} \mathbb{P}(p) \setminus \mathbb{P}(q) \text{ with } \left(\left(\frac{q}{l}\right)\right) = -1, \text{ or} \\ \mathbb{P}(q) \setminus \mathbb{P}(p) \text{ with } \left(\left(\frac{2p}{l}\right)\right) = \left(\left(\frac{-2p}{l}\right)\right) = -1, \text{ or} \\ \mathbb{P}(p) \cap \mathbb{P}(q) \text{ with } \left(\left(\frac{2pq}{l}\right)\right) = \left(\left(\frac{-2pq}{l}\right)\right) = -1 \end{cases}$$

In particular, if p is a prime $\equiv 1 \pmod{8}$ and q is a prime $\equiv 3 \pmod{8}$ with $\left(\frac{p}{q}\right) = -1$ then $\mathbb{Z}_{(p)} = R_{p,q}^{[1]}$.

Proof: (a) By Observation 5, $\Delta_{3,3} = \{2, 3\}$ and $\Delta_{2,5} = \{2, 5\}$, hence, by Lemma 6,

$$T_{3,3} + T_{2,5} = \bigcap_{l \in \Delta_{3,3} \cap \Delta_{2,5}} \mathbb{Z}_{(l)} = \mathbb{Z}_{(2)}.$$

(b) First assume $p \in \mathbb{Q}^\times$ with $p \equiv_2 3 \pmod{8}$. Then, by Observation 5,

$$\begin{aligned} \Delta_{-p,-p} \cap \mathbb{P} &= \mathbb{P}^{[3]}(p) \cup \mathbb{P}^{[7]}(p) \\ \Delta_{2p,-p} &= \mathbb{P}^{[3]}(p) \cup \mathbb{P}^{[5]}(p) \cup \{2\}, \end{aligned}$$

so $\Delta_{-p,-p} \cap \Delta_{2p,-p} = \mathbb{P}^{[3]}(p)$, and

$$R_P^{[3]} := T_{-p,-p} + T_{2p,-p} = \bigcap_{l \in \mathbb{P}^{[3]}(p)} \mathbb{Z}_{(l)} = \begin{cases} \bigcap_{l \in \mathbb{P}^{[3]}(p)} \mathbb{Z}_{(l)} & \text{if } \mathbb{P}^{[3]}(p) \neq \emptyset \\ \mathbb{Q} & \text{if } \mathbb{P}^{[3]}(p) = \emptyset. \end{cases}$$

If $p \not\equiv_2 3 \pmod{8}$, the only possible additional prime is 2 (e.g. if $p \equiv 5 \pmod{8}$).

If $p \equiv_2 5 \pmod{8}$ then, again by Observation 5,

$$\begin{aligned} \Delta_{-2p,-p} \cap \mathbb{P} &= \mathbb{P}^{[5]}(p) \cup \mathbb{P}^{[7]}(p) \\ \Delta_{2p,-p} &= \mathbb{P}^{[3]}(p) \cup \mathbb{P}^{[5]}(p) \cup \{2\}, \end{aligned}$$

so $\Delta_{-2p,-p} \cap \Delta_{2p,-p} = \mathbb{P}^{[5]}(p)$, and

$$R_P^{[5]} := T_{-2p,-p} + T_{2p,-p} = \bigcap_{l \in \mathbb{P}^{[5]}(p)} \mathbb{Z}_{(l)} = \begin{cases} \bigcap_{l \in \mathbb{P}^{[5]}(p)} \mathbb{Z}_{(l)} & \text{if } \mathbb{P}^{[5]}(p) \neq \emptyset \\ \mathbb{Q} & \text{if } \mathbb{P}^{[5]}(p) = \emptyset. \end{cases}$$

Again, the prime 2 (and no other prime) may or may not enter if $p \not\equiv_2 5 \pmod{8}$.

Finally, if $p \equiv_2 7 \pmod 8$ then, again by Observation 5,

$$\begin{aligned}\Delta_{-p,-p} \cap \mathbb{P} &= \mathbb{P}^{[3]}(p) \cup \mathbb{P}^{[7]}(p) \\ \Delta_{2p,p} \cap \mathbb{P} &= \mathbb{P}^{[5]}(p) \cup \mathbb{P}^{[7]}(p) \cup \{2\},\end{aligned}$$

so $\Delta_{-p,-p} \cap \Delta_{2p,p} = \mathbb{P}^{[7]}(p)$, and

$$R_p^{[7]} := T_{-p,-p} + T_{2p,p} = \bigcap_{l \in \mathbb{P}^{[7]}(p)} \mathbb{Z}_{(l)} = \begin{cases} \bigcap_{l \in \mathbb{P}^{[7]}(p)} \mathbb{Z}_{(l)} & \text{if } \mathbb{P}^{[7]}(p) \neq \emptyset \\ \mathbb{Q} & \text{if } \mathbb{P}^{[7]}(p) = \emptyset. \end{cases}$$

As before, 2 may enter if $p \not\equiv_2 7 \pmod 8$.

(c) Assume $p, q \in \mathbb{Q}^\times$ with $p \equiv_2 1 \pmod 8$ and $q \equiv_2 3 \pmod 8$. Then, once more using Observation 5,

$$\begin{aligned}\Delta_{2pq,q} \cap \mathbb{P} &= \{l \in \mathbb{P}(p) \setminus \mathbb{P}(q) \text{ with } \left(\left(\frac{q}{l}\right)\right) = -1\} \\ &\cup \{l \in \mathbb{P}(q) \setminus \mathbb{P}(p) \text{ with } \left(\left(\frac{-2p}{l}\right)\right) = -1\} \\ &\cup \{l \in \mathbb{P}(p) \cap \mathbb{P}(q) \text{ with } \left(\left(\frac{2pq}{l}\right)\right) = -1\} \\ \Delta_{-2pq,q} \cap \mathbb{P} &= \{l \in \mathbb{P}(p) \setminus \mathbb{P}(q) \text{ with } \left(\left(\frac{q}{l}\right)\right) = -1\} \\ &\cup \{l \in \mathbb{P}(q) \setminus \mathbb{P}(p) \text{ with } \left(\left(\frac{2p}{l}\right)\right) = -1\} \\ &\cup \{l \in \mathbb{P}(p) \cap \mathbb{P}(q) \text{ with } \left(\left(\frac{-2pq}{l}\right)\right) = -1\} \cup \{2\},\end{aligned}$$

which gives exactly the condition $\Delta_{2pq,q} \cap \Delta_{-2pq,q} = \mathbb{P}(p, q)$ needed to prove part (c) for $R_{p,q}^{[1]} := T_{2pq,q} + T_{-2pq,q}$. \square

Corollary 10.

$$\mathbb{Z} = \mathbb{Z}_{(2)} \cap \bigcap_{p,q \in \mathbb{Q}^\times} (R_p^{[3]} \cap R_p^{[5]} \cap R_p^{[7]} \cap R_{p,q}^{[1]})$$

Step 3: An existential definition of the Jacobson radical

We will show that, for some rings R occurring in Proposition 9, the Jacobson radical $J(R)$ can be defined by an existential formula. This will also give rise to new diophantine predicates in \mathbb{Q} .

Lemma 11. *Let $a, b \in \mathbb{Q}^\times$ and let*

$$J_{a,b} := \{x \in \mathbb{Q} \mid \exists y_1, y_2 \in \mathbb{Q} \text{ such that} \\ y_1, x - y_1 \in a \cdot \mathbb{Q}^2 \cdot T_{a,b}^\times \cap (1 - \mathbb{Q}^2 \cdot T_{a,b}^\times) \\ y_2, x - y_2 \in b \cdot \mathbb{Q}^2 \cdot T_{a,b}^\times \cap (1 - \mathbb{Q}^2 \cdot T_{a,b}^\times)\}.$$

Then $J_{a,b}$ is diophantine in \mathbb{Q} , and

$$J_{a,b} = \begin{cases} \bigcap_{l \in \Delta_{a,b} \setminus \{\infty\}} l \mathbb{Z}_l & \text{if } 2 \notin \Delta_{a,b} \neq \emptyset \\ \bigcap_{l \in \Delta_{a,b} \setminus \{\infty\}} l \mathbb{Z}_l & \text{if } 2 \in \Delta_{a,b} \text{ and } v_2(a) \text{ or } v_2(b) \text{ is odd} \\ \bigcap_{l \in \Delta_{a,b} \setminus \{2, \infty\}} l \mathbb{Z}_l & \text{if } 2 \in \Delta_{a,b} \not\subseteq \{2, \infty\} \text{ and } v_2(a), v_2(b) \text{ are even} \\ \mathbb{Q} & \text{otherwise} \end{cases}$$

Proof: Obviously, $J_{a,b}$ is diophantine in \mathbb{Q} , since this is true for the set \mathbb{Q}^2 of rational squares, for $T_{a,b}$, and hence for

$$T_{a,b}^\times := \{u \in T_{a,b} \mid \exists v \in T_{a,b} \text{ with } uv = 1\}$$

This is well-defined even if $T_{a,b}$ is not a ring, i.e. if $\infty \in \Delta_{a,b}$ in which case

$$T_{a,b}^\times = ([-4, -\frac{1}{4}] \cup [\frac{1}{4}, 4]) \cap \bigcap_{l \in \Delta_{a,b} \setminus \{\infty\}} \mathbb{Z}_{(l)}^\times.$$

For $a, b, c \in \mathbb{Q}^\times$, we define

$$I_{a,b}^c := \{y \in \mathbb{Q} \mid y, x - y \in c \cdot \mathbb{Q}^2 \cdot T_{a,b}^\times \cap (1 - \mathbb{Q}^2 \cdot T_{a,b}^\times)\}.$$

Note that

$$\mathbb{Q}^2 \cdot T_{a,b}^\times = \{0\} \cup \bigcap_{l \in \Delta_{a,b} \setminus \{\infty\}} v_l^{-1}(2\mathbb{Z}),$$

and so, by the ultrametric inequality,

$$I_{a,b}^c = \{y \in \mathbb{Q} \mid v_l(y) \text{ is odd and } > 0 \text{ for all } l \in \Delta_{a,b} \cap \mathbb{P}(c)\}.$$

(Recall from Definition 8 that $\mathbb{P}(c) := \{l \in \mathbb{P} \mid v_l(c) \text{ is odd}\}$.) By approximation, it follows that

$$I_{a,b}^c + I_{a,b}^c = \bigcap_{l \in \Delta_{a,b} \cap \mathbb{P}(c)} l \mathbb{Z}_{(l)},$$

where, as before, this intersection $= \mathbb{Q}$ in case $\Delta_{a,b} \cap \mathbb{P}(c) = \emptyset$.

Finally, observe that $J_{a,b} = (I_{a,b}^a + I_{a,b}^a) \cap (I_{a,b}^b + I_{a,b}^b)$ and apply Observation 5 to read off the various cases for $J_{a,b}$. \square

We can now give the existential definition of the Jacobson radical $J(R)$ for some of the rings R defined in Step 2 (cf. Definition 7 and Proposition 9):

Corollary 12. Define for $k = 1, 3, 5$ and 7 ,

$$\begin{aligned}\Phi_k &:= \{p \in \mathbb{Q}^\times \mid p \equiv_2 k \pmod{8} \text{ and } \mathbb{P}(p) \subseteq \mathbb{P}^{[1]} \cup \mathbb{P}^{[k]}\} \\ \Psi &:= \{(p, q) \in \Phi_1 \times \Phi_3 \mid p \in 2 \cdot (\mathbb{Q}^\times)^2 \cdot (1 + J(R_q^{[3]}))\}.\end{aligned}$$

(a) Then Φ_k is diophantine in \mathbb{Q} .

(b) The following implications hold for any $p \in \mathbb{Q}^\times$:

$$\begin{aligned}p \in \Phi_3 \text{ and } R_p^{[3]} &:= T_{-p, -p} + T_{2p, -p} \Rightarrow J(R_p^{[3]}) = J_{-p, -p} + J_{2p, -p} \neq \{0\} \\ p \in \Phi_5 \text{ and } R_p^{[5]} &:= T_{-2p, -p} + T_{2p, -p} \Rightarrow J(R_p^{[5]}) = J_{-2p, -p} + J_{2p, -p} \neq \{0\} \\ p \in \Phi_7 \text{ and } R_p^{[7]} &:= T_{-p, -p} + T_{2p, p} \Rightarrow J(R_p^{[7]}) = J_{-p, -p} + J_{2p, p} \neq \{0\}\end{aligned}$$

In particular, in each of the cases, the Jacobson radical is diophantine in \mathbb{Q} .

(c) Ψ is diophantine in \mathbb{Q} .

Proof: (a) It is clear from Proposition 9(a) that, for $k = 1, 3, 5$ and 7 , the property ‘ $p \equiv_2 k \pmod{8}$ ’ is diophantine.

Moreover, if $2 \notin \mathbb{P}(p)$ and $k = 3, 5$ or 7 , then, by Proposition 9,

$$\mathbb{P}^{[k]}(p) = \emptyset \iff p \in (\mathbb{Q}^\times)^2 \cdot (R_p^{[k]})^\times$$

So the property on the left is diophantine. But then so are

$$\begin{aligned}\Phi_1 &= \{p \equiv_2 1 \pmod{8} \mid \mathbb{P}_3(p) = \emptyset, \mathbb{P}_5(p) = \emptyset \text{ and } \mathbb{P}_7(p) = \emptyset\} \\ \Phi_3 &= \{p \equiv_2 3 \pmod{8} \mid \mathbb{P}_5(p) = \emptyset \text{ and } \mathbb{P}_7(p) = \emptyset\} \\ \Phi_5 &= \{p \equiv_2 5 \pmod{8} \mid \mathbb{P}_3(p) = \emptyset \text{ and } \mathbb{P}_7(p) = \emptyset\} \\ \Phi_7 &= \{p \equiv_2 7 \pmod{8} \mid \mathbb{P}_3(p) = \emptyset \text{ and } \mathbb{P}_5(p) = \emptyset\}.\end{aligned}$$

(b) For $k = 3, 5$ or 7 , ‘ $p \in \Phi_k$ ’ implies that $\mathbb{P}^{[k]}(p) \neq \emptyset$. From this, the assertion follows using Proposition 9(b) and Lemma 11.

(c) follows directly from (a) and (b). \square

The most difficult case is when $p \in \Phi_1$:

Proposition 13. Assume $(p, q) \in \Psi$. Then $R_{p,q}^{[1]} := T_{2pq,q} + T_{-2pq,q} \neq \mathbb{Q}$ and $J(R_{p,q}^{[1]}) = J_{2pq,q} + J_{-2pq,q}$, which, in particular, is diophantine in \mathbb{Q} .

Proof: Modulo square factors (which don’t change $R_{p,q}^{[1]}$) we can write

$$\begin{aligned}p &= p_1 \cdots p_m \cdot p_{m+1} \cdots p_n \\ q &= q_1 \cdots q_s \cdot p_1 \cdots p_m \cdot r_1 \cdots r_t,\end{aligned}$$

where the primes $p_i, r_k \in \mathbb{P}^{[1]}$ and $q_j \in \mathbb{P}^{[3]}$ are all distinct.

Then s is odd, as $q \equiv 3 \pmod{8}$. We may have $m = 0$ or $m = n$, but we always have $n \geq 1$: $p \in 2 \cdot (\mathbb{Q}^\times)^2 \cdot (1 + J(R_q^{[3]}))$, and so p is a non-square for all $l \in \mathbb{P}^{[3]}(q) = \{q_1, \dots, q_s\}$.

Now consider the following table of Legendre Symbols (and zeros):

	$q_1 \dots q_k \dots q_s$	$p_1 \dots p_j \dots p_m$	$r_1 \dots r_l \dots r_t$
p_1	$\left(\frac{q_k}{p_j}\right)$	0	$\left(\frac{r_l}{p_j}\right)$
\vdots			
p_j			
\vdots			
p_m			
p_{m+1}	$\left(\frac{q_k}{p_i}\right)$	$\left(\frac{p_j}{p_i}\right)$	$\left(\frac{r_k}{p_i}\right)$
\vdots			
p_i			
\vdots			
p_n			

and define

$$\begin{aligned}
\text{for } 1 \leq j \leq n : \quad & s_j := \#\{k \leq s \mid \left(\frac{q_k}{p_j}\right) = -1\} \\
& t_j := \#\{l \leq t \mid \left(\frac{r_l}{p_j}\right) = -1\} \\
\text{for } 1 \leq j \leq m : \quad & n'_j := \#\{i > m \mid \left(\frac{p_j}{p_i}\right) = -1\} \\
\text{for } m+1 \leq i \leq n : \quad & m_i := \#\{j \leq m \mid \left(\frac{p_j}{p_i}\right) = -1\} \\
\text{for } 1 \leq k \leq s : \quad & n_k := \#\{i \leq n \mid \left(\frac{q_k}{p_i}\right) = -1\} \\
\text{for } 1 \leq l \leq t : \quad & n_l^* := \#\{i \leq n \mid \left(\frac{r_l}{p_i}\right) = -1\}
\end{aligned}$$

Note that for all occurring Legendre symbols, top and bottom may be exchanged by the Quadratic Reciprocity Law.

Note also that, for $1 \leq k \leq s$, n_k is odd since p is a q_k -adic non-square. Hence $\sum_{k=1}^s n_k$ is odd.

Case 1 *There is some $j \leq m$ such that $s_j + t_j + n'_j$ is odd.*

In that case $p_j \in \mathbb{P}(p) \cap \mathbb{P}(q)$ with $\left(\left(\frac{2pq}{p_j}\right)\right) = \left(\left(\frac{-2pq}{p_j}\right)\right) = -1$.

Hence, by Proposition 9(c), $R_{p,q}^{[1]} \subseteq \mathbb{Z}_{(p_j)}$.

Case 2 *There is some $i \in \{m+1, \dots, n\}$ such that $s_i + m_i + t_i$ is odd.*

In that case $p_i \in \mathbb{P}(p) \setminus \mathbb{P}(q)$ with $\left(\left(\frac{q}{p_i}\right)\right) = -1$. Hence $R_{p,q}^{[1]} \subseteq \mathbb{Z}_{(p_i)}$.

Case 3 *There is some $l \leq t$ such that n_l^* is odd.*

In that case $r_l \in \mathbb{P}(q) \setminus \mathbb{P}(p)$ with $\left(\left(\frac{2p}{r_l}\right)\right) = \left(\left(\frac{-2p}{r_l}\right)\right) = -1$.

Hence $R_{p,q}^{[1]} \subseteq \mathbb{Z}_{(r_l)}$.

However, if all those numbers are even, then so is

$$\sum_{j=1}^m (s_j + t_j + n'_j) + \sum_{i=m+1}^n (s_i + m_i + t_i) + \sum_{l=1}^t n_l^* \quad (0)$$

It makes no difference whether we count the number of -1 's in each of the boxes rowwise or columnwise. Hence

$$\sum_{l=1}^t n_l^* = \sum_{j=1}^m t_j + \sum_{i=m+1}^n t_i \quad (1)$$

$$\sum_{j=1}^m n'_j = \sum_{i=m+1}^n m_i \quad (2)$$

$$\sum_{k=1}^s n_k = \sum_{j=1}^m s_j + \sum_{i=m+1}^n s_i \quad (3)$$

Plugging equations (1) and (2) into the sum (0) gives the sum

$$\sum_{j=1}^m s_j + \sum_{i=m+1}^n s_i + 2 \left(\sum_{j=1}^m t_j + \sum_{i=m+1}^n (m_i + t_j) \right)$$

which is still even. But then in equation (3), the right hand side is even while the left hand side is odd.

This contradiction shows that Case 1 or Case 2 or Case 3 must hold, and so the assertion follows. \square

Explicit formulas: For any $p \in \mathbb{Q}^\times$ with $2 \notin \mathbb{P}(p)$ and for $k = 3, 5$ or 7 , by the proof of Corollary 12(a),

$$\begin{aligned} \mathbb{P}^{[k]}(p) = \emptyset &\iff p \in \mathbb{Q}^2 \cdot (R_p^{[k]})^\times \\ &\iff \exists u, v \in R_p^{[k]} \exists w \in \mathbb{Q} (uw = 1 \wedge p = w^2 u) \\ &\iff \exists u, v, w, \bar{x}, \bar{y} \ h^{[k]}(p; u, v, w, \bar{x}, \bar{y}) = 0, \end{aligned}$$

where $\bar{x} = x_1, \dots, x_{15}$, $\bar{y} = y_1, \dots, y_{15}$ and

$$h^{[k]}(p; u, v, w, \bar{x}, \bar{y}) = f_p^{[k]}(u; \bar{x}) + f_p^{[k]}(v; \bar{y}) + (uv - 1)^2 + (w^2u - p)^2.$$

Here the $f_p^{[k]}$ are the polynomials introduced in Step 2 for the explicit diophantine formulas for the $R_p^{[k]}$'s. Note that the $f_p^{[k]}$'s are already sums of squares, so we don't have to square those again. Hence $h^{[k]}$ has degree 6 and 33 variables (besides p).

So from the formulas for Φ_k given in the proof of Corollary 12(a) one can find, using the $h^{[k]}$'s, polynomials $\phi_k \in \mathbb{Z}[p; \bar{z}]$ of degree 6 such that, for all $p \in \mathbb{Q}$ and for $k = 1, 3, 5$ or 7 ,

$$p \in \Phi_k \iff \exists \bar{z} \phi_k(p; \bar{z}) = 0,$$

where \bar{z} is a tuple of $15 + 33 + 33 = 81$ variables in case $k = 3, 5$ or 7 , and of $15 + 33 + 33 + 33 = 114$ variables for $k = 1$.

In order to find an explicit formula for Ψ , let us first observe that, for $k = 3, 5$ or 7 , for $p \in \Phi_k$ and for any $t \in \mathbb{Q}$,

$$t \in J(R_p^{[k]}) \iff t \in \left((R_p^{[k]} \cap p \cdot \mathbb{Q}^2 \cdot (R_p^{[k]})^\times) + (R_p^{[k]} \cap p \cdot \mathbb{Q}^2 \cdot (R_p^{[k]})^\times) \right),$$

so one finds polynomials $j^{[k]}(t, p; \bar{x})$ of degree 6, where the tuple \bar{x} has 97 variables such that

$$t \in J(R_p^{[k]}) \iff \exists \bar{x} j^{[k]}(t, p; \bar{x}) = 0.$$

(The definition of the $J(R_p^{[k]})$ as in Corollary 12(b) would require even more variables.)²

Looking at the definition of Ψ , it is now clear that we can find a polynomial $\psi(p, q; \bar{x})$ of degree 6 such that, for $p, q \in \mathbb{Q}$,

$$(p, q) \in \Psi \iff \exists \bar{x} \psi(p, q; \bar{x}) = 0,$$

where \bar{x} is a tuple of $114 + 81 + 99 = 294$ variables.

Finally, from Proposition 13 and Lemma 11, we see that there is a polynomial $j^{[1]} \in \mathbb{Z}[t, p, q; \bar{x}]$ of degree 6 such that for all $(p, q) \in \Psi$ and for all $t \in \mathbb{Q}$,

$$t \in J(R_{p,q}^{[1]}) \iff \exists \bar{x} j^{[1]}(t, p, q; \bar{x}) = 0.$$

Here \bar{x} is a tuple of 121 variables.

Step 4: From existential to universal³

Let R be a semilocal subring of \mathbb{Q} , i.e. $R = \bigcap_{l \in \Delta} \mathbb{Z}_{(l)}$ for some finite $\Delta \subseteq \mathbb{P}$. Define

$$\tilde{R} := \{x \in \mathbb{Q} \mid \neg \exists y \in J(R) \text{ with } x \cdot y = 1\}.$$

²We have the feeling that if one were to make a sport out of reducing the quantity of universal quantifiers in our definition for \mathbb{Z} in \mathbb{Q} it would be those J 's to jump on first.

³Converting an existential formula into a universal formula is locally (i.e. in \mathbb{R} and in \mathbb{Q}_p) always possible, by model completeness of these fields. That it works here globally as well is because our existential formulas mainly involve quadratic forms for which we have a local-global principle.

Lemma 14. (a) If $J(R)$ is diophantine in \mathbb{Q} then \tilde{R} is defined by a universal formula in \mathbb{Q} .

(b) $\tilde{R} = \bigcup_{l \in \Delta} \mathbb{Z}_{(l)}$, provided $\Delta \neq \emptyset$, i.e. provided $R \neq \mathbb{Q}$.

(c) In particular, if $R = \mathbb{Z}_{(p)}$ for some $p \in \mathbb{P}$ then $\tilde{R} = R$.

Proof: (a) is obvious from the definition of \tilde{R} , and (c) is a special case of (b). So we only need to prove (b).

For the inclusion ' \subseteq ', pick $x \in \tilde{R}$ and assume that $x \notin \bigcup_{l \in \Delta} \mathbb{Z}_{(l)}$. Then for all $l \in \Delta$, $v_l(x) < 0$, and hence $y := x^{-1} \in \bigcap_{l \in \Delta} l\mathbb{Z}_{(l)} = J(R)$, contradicting our assumption that $x \in \tilde{R}$.

For the converse inclusion ' \supseteq ', assume $x \in \mathbb{Z}_{(l)}$ for some $l \in \Delta$. Then, for any $y \in J(R)$, $x \cdot y \in l\mathbb{Z}_{(l)}$, so, in particular $x \cdot y \neq 1$. \square

Now we can give our universal definition of \mathbb{Z} in \mathbb{Q} :

Proposition 15. (a)

$$\mathbb{Z} = \widetilde{\mathbb{Z}_{(2)}} \cap \left(\bigcap_{k=3,5,7} \bigcap_{p \in \Phi_k} \widetilde{R_p^{[k]}} \right) \cap \bigcap_{(p,q) \in \Psi} \widetilde{R_{p,q}^{[1]}},$$

where Φ_k and Ψ are the diophantine sets defined in Corollary 12.

(b) for any $t \in \mathbb{Q}$,

$$\begin{aligned} t \in \mathbb{Z} \iff & t \in \widetilde{\mathbb{Z}_{(2)}} \wedge \\ & \forall p \bigwedge_{k=3,5,7} (t \in \widetilde{R_p^{[k]}} \vee p \notin \Phi_k) \wedge \\ & \forall p, q (t \in \widetilde{R_{p,q}^{[1]}} \vee (p, q) \notin \Psi) \end{aligned}$$

(c) (**Theorem 1**) There is a polynomial $g \in \mathbb{Z}[t; x_1, \dots, x_{418}]$ of degree 28 such that, for any $t \in \mathbb{Q}$,

$$t \in \mathbb{Z} \text{ iff } \forall x_1 \dots \forall x_{418} \in \mathbb{Q} \ g(t; x_1, \dots, x_{418}) \neq 0.$$

Proof: (a) The equation is valid by Proposition 9, Lemma 14(b), (c).

(b) is a reformulation of (a) revealing that the formula thus obtained for \mathbb{Z} in \mathbb{Q} is universal: the \tilde{R} 's are universal by Corollary 12, Proposition 13 and Lemma 14(a); Φ_k and Ψ are existential by Corollary 12(a) and (c), so their negation is universal as well.

(c) Here we use the explicit formulas from the end of Step 3 to find the polynomial: Note that if $J(R)$ was defined with n existential quantifiers then \tilde{R} is defined with $n + 1$ universal quantifiers. Also, as in Step 2, $\mathbb{Z}_{(2)} = T_{3,3} + T_{2,5}$ has a diophantine definition where the defining polynomial $f_2(t; \bar{x})$ has degree 4 (and \bar{x} has 15 variables), so the same is true for the defining polynomial $j_2(t; \bar{x})$ of $J(\mathbb{Z}_{(2)}) = 2\mathbb{Z}_{(2)}$.

Putting things together, the polynomial is

$$\begin{aligned} g(t; p, q, \bar{x}) &:= (j_2(x_1; \overline{2x^{15}}) + (tx_1 - 1)^2) \\ &\quad \cdot \prod_{k=3,5,7} \left(j^{[k]}(x_1; \overline{2x^{98}}) + (tx_1 - 1)^2 + \phi_k(p; \overline{101x^{181}}) \right) \\ &\quad \cdot \left(j^{[1]}(x_1, p, q; \overline{2x^{122}}) + (tx_1 - 1)^2 + \psi(p, q; \overline{123x^{416}}) \right) \end{aligned}$$

where \bar{x} is the tuple x_1, \dots, x_{416} , and where we use $\overline{mx^n}$ to denote the tuple x_m, x_{m+1}, \dots, x_n . Note again, that all occurring j, ϕ, ψ are sums of squares of polynomials, so there is no need to square them once more. \square

3 More diophantine predicates in \mathbb{Q}

From the results and techniques of section 2, one obtains new diophantine predicates in \mathbb{Q} . They are of interest in their own right, but maybe they can also be used to show that Hilbert's 10th problem cannot be solved, not by defining or interpreting \mathbb{Z} in \mathbb{Q} , but by assigning graphs to the various finite sets of primes encoded in these predicates, and using graph theoretic undecidability results. We will also use some of these new predicates for our $\forall\exists$ -definition of \mathbb{Z} in \mathbb{Q} which uses just one universal quantifier (Corollary 18).

Before listing the new diophantine predicates we shall first prove the following

Lemma 16. *Assume $p \in \Phi_1 \setminus \mathbb{Q}^2$ and define*

$$R_p^{[1]} := \{x \in \mathbb{Q} \mid \exists q \text{ with } (p, q) \in \Psi, q \in (R_{p,q}^{[1]})^\times \text{ and } x \in R_{p,q}^{[1]}\}.$$

Then $R_p^{[1]}$ is diophantine in \mathbb{Q} and $R_p^{[1]} = \bigcup_{l \in \mathbb{P}(p)} \mathbb{Z}_{(l)}$.

In particular, if p is a prime $\equiv 1 \pmod{8}$ then $R_p^{[1]} = \mathbb{Z}_{(p)}$.

Let us mention (without proof) that our definition of $R_p^{[1]}$ requires 342 existential quantifiers.

Proof: That $R_p^{[1]}$ is diophantine in \mathbb{Q} is immediate from Corollary 12.

The condition ' $q \in (R_{p,q}^{[1]})^\times$ ' implies that, in the terminology of Proposition 9(c), $\mathbb{P}(p, q) \subseteq \mathbb{P}(p)$. Moreover, by Proposition 13, ' $(p, q) \in \Psi$ ' implies that $\mathbb{P}(p, q) \neq \emptyset$. Hence

$$R_p^{[1]} \subseteq \bigcup_{\substack{q \in (R_{p,q}^{[1]})^\times \text{ with} \\ (p, q) \in \Psi}} R_{p,q}^{[1]} \subseteq \bigcup_{\substack{q \in (R_{p,q}^{[1]})^\times \text{ with} \\ (p, q) \in \Psi}} \bigcap_{l \in \mathbb{P}(p, q)} \mathbb{Z}_{(l)} \subseteq \bigcup_{l \in \mathbb{P}(p)} \mathbb{Z}_{(l)}.$$

Conversely, pick $x \in \mathbb{Z}_{(l)}$ for some $l \in \mathbb{P}(p)$. Choose a prime $q \equiv 3 \pmod{8}$ with $\left(\frac{l}{q}\right) = -1$ and with $\left(\frac{l'}{q}\right) = 1$ for each $l' \in \mathbb{P}(p) \setminus \{l\}$.

Then $\left(\left(\frac{p}{q}\right)\right) = -1$, so $(p, q) \in \Psi$. Hence, by Proposition 9(c) and the Quadratic Reciprocity Law, $\mathbb{P}(p, q) = \{l\}$. Thus $x \in \mathbb{Z}_{(l)} = R_{p,q}^{[1]}$ and $q \in (R_{p,q}^{[1]})^\times$, i.e. $x \in R_p^{[1]}$. \square

Proposition 17. *For $x, y \in \mathbb{Q}^\times$, the following properties are diophantine:*

- (a) *For $k = 3, 5$ or 7 : $x, y \in \Phi_k$ and $\mathbb{P}^{[k]}(x) \cap \mathbb{P}^{[k]}(y) = \emptyset$*
- (b) *$x \notin \mathbb{Q}^2$*
- (c) *For $k = 1, 3, 5$ or 7 : $x \equiv_2 k \pmod{8}$ and $x \notin \Phi_k$*
- (d) *For $k = 3, 5$ or 7 : $\mathbb{P}^{[k]}(x) = \emptyset$*
- (e) *$x \notin N(y)$, where $N(y)$ is the image of the norm $\mathbb{Q}(\sqrt{y}) \rightarrow \mathbb{Q}$*

Again, we mention (without proof) the number of existential quantifiers one would use if one were to spell out the formulas resulting from our diophantine descriptions: for (a): 195 for (c): 1077 if $k = 1$ for (d): 558
for (b): 181 1373 if $k = 3, 5, 7$ for (e): 450

Along similar lines (also without proof here) one finds other diophantine properties involving the $\mathbb{P}^{[k]}$ -predicates (for $k = 1, 3, 5, 7$), e.g.

$$\mathbb{P}^{[k]}(x) \neq \emptyset, \mathbb{P}^{[k]}(x) \subseteq \mathbb{P}^{[k]}(y), \mathbb{P}^{[k]}(x) \subsetneq \mathbb{P}^{[k]}(y), \#\mathbb{P}^{[k]}(x) = n \text{ for } n \in \mathbb{N} \text{ etc.}$$

Proof: (a) By Corollary 12(a), Φ_k is diophantine. For any $x \in \Phi_k$, $\mathbb{P}^{[k]}(x) \neq \emptyset$ and hence, by Corollary 12(b), $J(R_x^{[k]})$ is diophantine. The equivalence

$$\mathbb{P}^{[k]}(x) \cap \mathbb{P}^{[k]}(y) = \emptyset \iff 1 \in J(R_x^{[k]}) + J(R_y^{[k]})$$

for $x, y \in \Phi_k$ then proves **(a)**, using Corollary 12(b).

(b) By Lemma 9(a), the property that ' $v_2(x)$ is odd' is diophantine, as is the property ' $x < 0$ '. Hence, again with Corollary 12(a) and (b), it suffices to show

$$x \notin \mathbb{Q}^2 \iff \begin{cases} x < 0 \text{ or } v_2(x) \text{ is odd or} \\ \exists p \in \Phi_3 \text{ with } x \in 2 \cdot (\mathbb{Q}^\times)^2 \cdot (1 + J(R_p^{[3]})) \end{cases}$$

' \Rightarrow ': Assume that $x \notin \mathbb{Q}^2$, that $x > 0$ and that $v_2(x)$ is even. Then, modulo squares, $x = p_1 \cdots p_r$ for distinct odd primes p_1, \dots, p_r .

$$\text{Choose } a_1 \in \mathbb{Z} \text{ with } \left(\frac{a_1}{p_1} \right) = \begin{cases} -1 & \text{if } p_1 \equiv 1 \pmod{4} \\ 1 & \text{if } p_1 \equiv 3 \pmod{4} \end{cases}$$

and, for $i > 1$,

$$\text{choose } a_i \in \mathbb{Z} \text{ with } \left(\frac{a_i}{p_i} \right) = \begin{cases} 1 & \text{if } p_i \equiv 1 \pmod{4} \\ -1 & \text{if } p_i \equiv 3 \pmod{4} \end{cases}$$

Finally, choose a prime $p \equiv 3 \pmod{8}$ with $p \equiv a_i \pmod{p_i}$ ($i = 1, \dots, r$).

Then, by the Quadratic Reciprocity Law, $\left(\frac{x}{p} \right) = -1$.

Clearly, $p \in \Phi_3$. By Lemma 9(b), $R_p^{[3]} = \mathbb{Z}_{(p)}$. Hence $x \in 2 \cdot (\mathbb{Q}^\times)^2 \cdot (1 + J(R_p^{[3]}))$.

' \Leftarrow ': If $x < 0$ or $v_2(x)$ is odd then clearly $x \notin \mathbb{Q}^2$.

If $x \in 2 \cdot (\mathbb{Q}^\times)^2 \cdot (1 + J(R_p^{[3]}))$ for some $p \in \Phi_3$ then $\mathbb{P}^{[3]}(p) \neq \emptyset$, and for any $l \in \mathbb{P}^{[3]}(p)$ one has $\left(\left(\frac{x}{l} \right) \right) = \left(\frac{2}{l} \right) = -1$. Hence $x \notin \mathbb{Q}^2$.

(c) First assume $x \equiv_2 1 \pmod{8}$. Then $x \notin \Phi_1$ iff

$$\begin{aligned} & \exists y_3, y'_3, y_5, y'_5, y_7, y'_7 \\ & \bigwedge_{k=3,5,7} (y_k, y'_k \in \Phi_k \wedge \mathbb{P}^{[k]}(y_k) \cap \mathbb{P}^{[k]}(y'_k) = \emptyset) \\ & \wedge \left(\bigvee_{k=3,5,7} x = y_k y'_k \vee \bigvee_{k \neq l \in \{3,5,7\}} x = y_k y'_k y_l y'_l \vee x = y_3 y_5 y_7 \vee x = y_3 y'_3 y_5 y'_5 y_7 y'_7 \right) \end{aligned}$$

This is diophantine by part (a) and by Corollary 12(a).

Now assume $x \equiv_2 3 \pmod{8}$. Then $x \notin \Phi_3$ iff

$$\begin{aligned} & \exists y_1, y_3, y'_3, y_5, y'_5, y_7, y'_7 \\ & \left(y_1 \in \Phi_1 \wedge y_1 \notin \mathbb{Q}^2 \wedge \bigwedge_{k=3,5,7} (y_k, y'_k \in \Phi_k \wedge \mathbb{P}^{[k]}(y_k) \cap \mathbb{P}^{[k]}(y'_k) = \emptyset) \right) \\ & \wedge \left\{ \begin{aligned} & x = y_1 y_3 \vee x = y_5 y_7 \vee x = y_3 y_5 y'_5 \vee x = y_3 y_7 y'_7 \vee x = y_1 y_5 y_7 \\ & \vee x = y_1 y_3 y_5 y'_5 \vee x = y_1 y_3 y_7 y'_7 \vee x = y_3 y'_3 y_5 y_7 \\ & \vee x = y_1 y_3 y'_3 y_5 y_7 \vee x = y_3 y_5 y'_5 y_7 y'_7 \vee x = y_1 y_3 y'_3 y_5 y_7 \vee x = y_1 y_3 y_5 y'_5 y_7 y'_7 \end{aligned} \right\} \end{aligned}$$

Note that the condition ' $y_1 \in \Phi_1 \setminus \mathbb{Q}^2$ ' guarantees that $\mathbb{P}^{[1]}(y_1) \neq \emptyset$.

Again, this is diophantine by parts (a), (b) and Corollary 12(a).

It is clear how similar existential formulas can be written down for ' $x \notin \Phi_5$ ' and ' $x \notin \Phi_7$ '.

(d) $\mathbb{P}^{[3]}(x) = \emptyset$ iff

$$\exists y_1, \dots, y_6 \left(y_1, y_2 \in \Phi_1 \wedge y_3, y_4 \in \Phi_5 \wedge y_5, y_6 \in \Phi_7 \wedge \bigvee_{\emptyset \neq I \subseteq \{1, \dots, 6\}} x = \prod_{i \in I} y_i \right)$$

And, again, similar formulas hold for $k = 5$ and $k = 7$.

(e) $x \notin N(y)$ iff

$$\begin{aligned} & (x < 0 \wedge y < 0) \\ & \vee \bigvee_{3,5,7} \exists p \in \Phi_k \text{ with} \\ & \left(\left(x \in p \cdot (\mathbb{Q}^\times)^2 \cdot (R_p^{[k]})^\times \right) \wedge \left(y \text{ or } xy \in a_k \cdot (\mathbb{Q}^\times)^2 \cdot (1 + J(R_p^{[k]})) \right) \right. \\ & \left. \vee \left(y \in p \cdot (\mathbb{Q}^\times)^2 \cdot (R_p^{[k]})^\times \right) \wedge \left(x \text{ or } xy \in a_k \cdot (\mathbb{Q}^\times)^2 \cdot (1 + J(R_p^{[k]})) \right) \right) \\ & \vee \exists (p, q) \in \Psi \text{ with } q \in (R_{p,q}^{[1]})^\times \text{ and} \\ & \left(\left(x \in p \cdot (\mathbb{Q}^\times)^2 \cdot (R_{p,q}^{[1]})^\times \right) \wedge \left(y \text{ or } xy \in q \cdot (\mathbb{Q}^\times)^2 \cdot (1 + J(R_{p,q}^{[1]})) \right) \right. \\ & \left. \vee \left(y \in p \cdot (\mathbb{Q}^\times)^2 \cdot (R_{p,q}^{[1]})^\times \right) \wedge \left(x \text{ or } xy \in q \cdot (\mathbb{Q}^\times)^2 \cdot (1 + J(R_{p,q}^{[1]})) \right) \right) \end{aligned}$$

where $a_3 = a_5 = 2$ and $a_7 = -1$.

This uses Observation 5(b) and (c), Corollary 12(b) and (c), the previous parts and the local-global principle for norms.

The first line says that $x \notin N(y)$ over \mathbb{R} .

Lines 2-4 say that $x \notin N(y)$ over \mathbb{Q}_l for some non-empty set of primes $l \equiv 3, 5 \text{ or } 7 \pmod{8}$.

Lines 5-7 say that $x \notin N(y)$ over \mathbb{Q}_l for some non-empty set of primes $l \equiv 1 \pmod{8}$. As in the proof of Lemma 16, the condition ' $q \in (R_{p,q}^{[1]})^\times$ ' makes sure that, in the terminology of Proposition 9(c), $\mathbb{P}(p, q) \cap \mathbb{P}(q) = \emptyset$, so $\mathbb{P}(p, q) \subseteq \mathbb{P}(q)$. And, by Proposition 13, $\mathbb{P}(p, q) \neq \emptyset$. Line 6 and 7 then say that $x \notin N(y)$ over \mathbb{Q}_l for any $l \in \mathbb{P}(p, q)$.

We could disregard the prime $p = 2$, as ' $x \notin N(y)$ ' either happens nowhere locally, or at least at two primes in $\mathbb{P} \cup \{\infty\}$. \square

(b) was also obtained in [P2] – using a deep result on Châtelet surfaces from [CSS] – our proof is elementary.

Let us also mention that (b) follows from (e): $x \notin \mathbb{Q}^2 \Leftrightarrow \exists y \ x \notin N(y)$ (and we did not use (b) in order to prove (e)).

We close this section by showing that there is an $\forall\exists$ -definition of \mathbb{Z} in \mathbb{Q} with just one universal quantifier (such a definition was independently given by Alexandra Shlapentokh using an entirely different elliptic curve method in [Sh]):

Corollary 18. *For all $t \in \mathbb{Q}$, $t \in \mathbb{Z}$ iff*

$$\forall p \left(t \in \mathbb{Z}_{(2)} \wedge \left\{ \begin{array}{l} \bigvee_{k=2,4,6} (p \in \mathbb{Q}^2 \cdot (k + 8\mathbb{Z}_{(2)})) \\ \vee \bigvee_{k=1,3,5,7} \left\{ \begin{array}{l} (p \neq 0 \wedge p \in \mathbb{Q}^2 \cdot (k + 8\mathbb{Z}_{(2)})) \\ \wedge \left((p \notin \Phi_k) \vee (p \in \Phi_k \setminus \mathbb{Q}^2 \wedge t \in R_p^{[k]}) \right) \end{array} \right\} \end{array} \right. \right)$$

Proof: The equivalence holds by Proposition 9(a) and (b) and by Lemma 16.

That the resulting formula is of the shape $\forall\exists$ with just one universal quantifier ‘ $\forall p$ ’ follows from Proposition 9, Corollary 12, Lemma 16 and Proposition 17. \square

Writing the formula in prenex normal form gives a formula with one universal and 1109 existential quantifiers.

4 Why \mathbb{Z} should not be diophantine in \mathbb{Q}

In this section we employ a model-theoretic construction in order to show that \mathbb{Z} is not diophantine in \mathbb{Q} , provided one believes in a certain version of the Bombieri-Lang Conjecture on varieties with many rational points.

The version of the Bombieri-Lang Conjecture in the special case of varieties over \mathbb{Q} on which our result is based is the following (mainly after [HS]):

Bombieri-Lang Conjecture *Let V be an absolutely irreducible affine or projective ≥ 1 -dimensional variety over \mathbb{Q} such that $V(\mathbb{Q})$ is \mathbb{Q} -Zariski dense in V . Then so is*

$$\bigcup_{\phi: A \dashrightarrow V} \phi(A(\mathbb{Q})),$$

where the $\phi : A \dashrightarrow V$ run through all non-trivial \mathbb{Q} -rational maps from ≥ 1 -dimensional abelian varieties A defined over \mathbb{Q} to V .

In Lang’s *Number Theory III*, the requirement that A and ϕ be defined over \mathbb{Q} is explicitly *not* made. This is, however, in order to arrive at the stronger conclusion that the complement of the k -Zariski closure of $\bigcup_{\phi: A \dashrightarrow V} \phi(A(k))$ in $V(k)$ be finite for all fields k finitely generated over \mathbb{Q} .

Let us also point out that our reading of ‘non-trivial’ in the Conjecture implies that there are such $\phi : A \dashrightarrow V$ over \mathbb{Q} for which $\phi(A(\mathbb{Q}))$ is infinite

(it is certainly in the spirit of the conjecture that the $\phi(A(\mathbb{Q}))$ account for $V(\mathbb{Q})$ being dense in V , but, strictly speaking, this reading gives a slightly stronger, though equally plausible, conjecture).

With this understanding let us first prove the following

Lemma 19. *Assume the Bombieri-Lang Conjecture as above. Let $V = V(f) \subseteq \mathbb{A}^{n+1}$ be an absolutely irreducible affine hypersurface defined over \mathbb{Q} such that $V(\mathbb{Q})$ is \mathbb{Q} -Zariski dense in V . Let $\pi : \mathbb{A}^{n+1} \rightarrow \mathbb{A}^1$ be a \mathbb{Q} -linear projection. Then $V(\mathbb{Q}) \cap \pi^{-1}(\mathbb{Q} \setminus \mathbb{Z})$ is also \mathbb{Q} -Zariski dense in V .*

(For $n = 1$ the Lemma holds unconditionally, by Siegel's Theorem.)

Proof: Choose any $g \in \mathbb{Q}[x_1, \dots, x_n] \setminus \{0\}$. By the Bombieri-Lang Conjecture there is an abelian variety A and a rational map $\phi : A \dashrightarrow V$, both defined over \mathbb{Q} , such that $\phi(A(\mathbb{Q})) \setminus V(g)(\mathbb{Q})$ is infinite (considering $V(g)$ as subset of \mathbb{A}^{n+1}). By possibly composing ϕ with another rational map, we may assume that $\pi(\phi(A(\mathbb{Q})) \setminus V(g)(\mathbb{Q}))$ is infinite, and that the pole divisor D of $\pi \circ \phi$ is ample. By Corollary 6.2 in [F], there are only finitely many $P \in A(\mathbb{Q}) \setminus D(\mathbb{Q})$ with $\pi(\phi(P)) \in \mathbb{Z}$ (cf. the remarks following Theorem 1 in [Si]). This implies that $(V(\mathbb{Q}) \setminus V(g)(\mathbb{Q})) \cap \pi^{-1}(\mathbb{Q} \setminus \mathbb{Z}) \neq \emptyset$. Since g was arbitrary this shows that $V(\mathbb{Q}) \cap \pi^{-1}(\mathbb{Q} \setminus \mathbb{Z})$ is \mathbb{Q} -Zariski dense in V . \square

Theorem 20. *Assume the Bombieri-Lang Conjecture as stated above. Then there is no infinite subset of \mathbb{Z} existentially definable in \mathbb{Q} . In particular, \mathbb{Z} is not diophantine in \mathbb{Q} .*

Proof: Suppose $A \subseteq \mathbb{Z}$ is infinite and definable in \mathbb{Q} by an existential formula $\phi_A(x)$ in the language of rings.

Choose a countable elementary proper extension \mathbb{Q}^* of \mathbb{Q} and let $A^* = \{x \in \mathbb{Q}^* \mid \phi_A(x)\}$. Then \mathbb{Q}^* contains some nonstandard natural number $x \in \mathbb{N}^* \setminus \mathbb{N}$. The map $\begin{cases} \mathbb{N} & \rightarrow \mathbb{N} \\ n & \mapsto 2^n \end{cases}$ is definable in \mathbb{N} and hence in \mathbb{Q} , so $2^x \in \mathbb{N}^*$. As 2^x is greater than any element algebraic over $\mathbb{Q}(x)$, the elements $x, 2^x, 2^{2^x}, \dots$ are algebraically independent over \mathbb{Q} . We therefore find an infinite countable transcendence base x_1, x_2, \dots of \mathbb{Q}^* over \mathbb{Q} . And, by realizing the type $\{\phi_A(x) \wedge x \neq a \mid a \in A\}$, we may assume that $x_1 \in A^*$ (here we use that A is infinite).

Let $K = \mathbb{Q}(x_1, x_2, \dots)$. As \mathbb{Q}^* is countable we find $\alpha_i \in \mathbb{Q}^*$ ($i \in \mathbb{N}$) such that

$$K(\alpha_1) \subseteq K(\alpha_2) \subseteq \dots \text{ with } \bigcup_{i=1}^{\infty} K(\alpha_i) = \mathbb{Q}^*,$$

where we may in addition assume that, for each $i \in \mathbb{N}$, the minimal polynomial $f_i \in K[z]$ of α_i over K has coefficients in $\mathbb{Q}[x_1, \dots, x_i]$. As \mathbb{Q} is relatively algebraically closed in \mathbb{Q}^* , all the $f_i \in \mathbb{Q}[x_1, \dots, x_i, z]$ are absolutely irreducible over \mathbb{Q} .

Now consider the following set of formulas in the free variables x_1, x_2, \dots :

$$\begin{aligned} p = p(x_1, x_2, \dots) \quad := \quad & \{g(x_1, \dots, x_i) \neq 0 \mid i \in \mathbb{N}, g \in \mathbb{Q}[x_1, \dots, x_i] \setminus \{0\}\} \\ & \cup \{\exists z f_i(x_1, \dots, x_i, z) = 0 \mid i \in \mathbb{N}\} \\ & \cup \{x_1 \text{ is not an integer}\} \end{aligned}$$

Then p is finitely realizable in \mathbb{Q} : Let $p_0 \subseteq p$ be finite and let i be the highest index occurring in p_0 among the formulas from line 2. Since the $K(\alpha_j)$ are linearly ordered by inclusion all formulas from line 2 with index $< i$ follow from the one with index i . Hence one only has to check that $V(f_i)$ has \mathbb{Q} -Zariski dense many \mathbb{Q} -rational points $(x_1, \dots, x_i, z) \in \mathbb{A}^{i+1}$ with $x_1 \notin \mathbb{Z}$. But this is, assuming the Bombieri-Lang Conjecture, exactly the conclusion of the above Lemma. Note that $V(f_i)(\mathbb{Q})$ is \mathbb{Q} -Zariski dense in $V(f_i)$ because there is a point $(x_1, \dots, x_i, \alpha_i) \in V(f_i)(\mathbb{Q}^*)$ with x_1, \dots, x_i algebraically independent over \mathbb{Q} .

Hence p is a type that we can realize in some elementary extension \mathbb{Q}^{**} of \mathbb{Q} . Calling the realizing ω -tuple in \mathbb{Q}^{**} again x_1, x_2, \dots our construction yields that we may view \mathbb{Q}^* as a subfield of \mathbb{Q}^{**} .

But now $x_1 \in A^* \subseteq \mathbb{Z}^*$ and $x_1 \notin \mathbb{Z}^{**}$, hence $x_1 \notin A^{**}$. This implies that there is after all no existential definition for A in \mathbb{Q} . \square

Let us conclude with a collection of closure properties of pairs of models of $\text{Th}(\mathbb{Q})$ (in the ring language), one a substructure of the other, which might have a bearing on the final (unconditional) answer to the question whether or not \mathbb{Z} is diophantine in \mathbb{Q} .

Proposition 21. *Let $\mathbb{Q}^*, \mathbb{Q}^{**}$ be models of $\text{Th}(\mathbb{Q})$ (i.e. elementary extensions of \mathbb{Q}) with $\mathbb{Q}^* \subseteq \mathbb{Q}^{**}$, and let \mathbb{Z}^* and \mathbb{Z}^{**} be their rings of integers. Then*

- (a) $\mathbb{Z}^{**} \cap \mathbb{Q}^* \subseteq \mathbb{Z}^*$.
- (b) $\mathbb{Z}^{**} \cap \mathbb{Q}^*$ is integrally closed in \mathbb{Q}^* .
- (c) $(\mathbb{Q}^{**})^2 \cap \mathbb{Q}^* = (\mathbb{Q}^*)^2$, i.e. \mathbb{Q}^* is quadratically closed in \mathbb{Q}^{**} .
- (d) If \mathbb{Z} is diophantine in \mathbb{Q} then $\mathbb{Z}^{**} \cap \mathbb{Q}^* = \mathbb{Z}^*$ and \mathbb{Q}^* is algebraically closed in \mathbb{Q}^{**} .

(e) \mathbb{Q} is not model complete, i.e., in general, \mathbb{Q}^* is not existentially closed in \mathbb{Q}^{**} .

Proof: (a) is an immediate consequence of our universal definition of \mathbb{Z} in \mathbb{Q} . The very same definition holds for \mathbb{Z}^* in \mathbb{Q}^* and for \mathbb{Z}^{**} in \mathbb{Q}^{**} (it is part of $\text{Th}(\mathbb{Q})$ that all definitions of \mathbb{Z} in \mathbb{Q} are equivalent). So if this universal formula holds for $x \in \mathbb{Z}^{**} \cap \mathbb{Q}^*$ in \mathbb{Q}^{**} it also holds in \mathbb{Q}^* , i.e. $x \in \mathbb{Z}^*$.

(b) is true because \mathbb{Z}^{**} is integrally closed in \mathbb{Q}^{**} .

(c) follows from the fact that both being a square and, by Proposition 17(b), not being a square are diophantine in \mathbb{Q} .

(d) If \mathbb{Z} is diophantine in \mathbb{Q} then $\mathbb{Z}^{**} \cap \mathbb{Q}^* \supseteq \mathbb{Z}^*$ and hence equality holds, by (a).

To show that then also \mathbb{Q}^* is algebraically closed in \mathbb{Q}^{**} , let us observe that, for each $n \in \mathbb{N}$,

$$A_n := \{(a_0, \dots, a_{n-1}) \in \mathbb{Z}^n \mid \exists x \in \mathbb{Z} \text{ with } x^n + a_{n-1}x^{n-1} + \dots + a_0 = 0\}$$

is decidable: zeros of polynomials in one variable are bounded in terms of their coefficients, so one only has to check finitely many $x \in \mathbb{Z}$. In particular, by (for short) Matiyasevich's Theorem, there is an \exists -formula $\phi(t_0, \dots, t_{n-1})$ such that

$$\mathbb{Z} \models \forall t_0 \dots t_{n-1} \forall x (x^n + t_{n-1}x^{n-1} + \dots + t_0 \neq 0 \leftrightarrow \phi(t_0, \dots, t_{n-1})).$$

Since both A_n and its complement in \mathbb{Z}^n are diophantine in \mathbb{Z} , the same holds in \mathbb{Q} , by our assumption of \mathbb{Z} being diophantine in \mathbb{Q} , i.e. $A_n^{**} \cap (\mathbb{Q}^*)^n = A^*$. As any finite extension of \mathbb{Q}^* is generated by an integral primitive element this implies that \mathbb{Q}^* is relatively algebraically closed in \mathbb{Q}^{**} .

(e) Choose a recursively enumerable subset $A \subseteq \mathbb{Z}$ which is not decidable. Then $B := \mathbb{Z} \setminus A$ is definable in \mathbb{Z} , and hence in \mathbb{Q} . If B were diophantine in \mathbb{Q} it would be recursively enumerable. But then A would be decidable: contradiction.

So not every definable subset of \mathbb{Q} is diophantine in \mathbb{Q} , and hence \mathbb{Q} is not model complete. Or, in other words, there are models $\mathbb{Q}^*, \mathbb{Q}^{**}$ of $\text{Th}(\mathbb{Q})$ with $\mathbb{Q}^* \subseteq \mathbb{Q}^{**}$ where \mathbb{Q}^* is not existentially closed in \mathbb{Q}^{**} . \square

We are confident that with similar methods as used in this paper one can show for an arbitrary prime p that the unary predicate ' $x \notin \mathbb{Q}^p$ ' is also diophantine. This would imply that, in the setting of the Proposition, \mathbb{Q}^* is always radically closed in \mathbb{Q}^{**} . However, we have no bias towards an answer (let alone an answer) to the following (unconditional)

Question 22. For $\mathbb{Q}^* \equiv \mathbb{Q}^{**} \equiv \mathbb{Q}$ with $\mathbb{Q}^* \subseteq \mathbb{Q}^{**}$, is \mathbb{Q}^* always algebraically closed in \mathbb{Q}^{**} ?

Appendix: Some duadic computations

$2, 3, 5$ is an \mathbb{F}_2 -basis for $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$. Denoting by $N(x)$ the image of the norm map $\mathbb{Q}_2(\sqrt{x})^\times \rightarrow \mathbb{Q}_2^\times$ and denoting by $\langle a, b \rangle$ the subgroup of \mathbb{Q}_2^\times generated by $(\mathbb{Q}_2^\times)^2$ and a and b , one has

$$\begin{aligned} N(2) &= \langle 2, 15 \rangle \\ N(3) &= \langle 5, 6 \rangle \\ N(5) &= \langle 3, 5 \rangle \\ N(6) &= \langle 3, 10 \rangle \\ N(10) &= \langle 6, 10 \rangle \\ N(15) &= \langle 2, 5 \rangle \\ N(30) &= \langle 2, 3 \rangle \end{aligned}$$

This is straightforward to check, using that $1 + 8\mathbb{Z}_2 \subseteq (\mathbb{Q}_2^\times)^2$.

From this one can read off all 16 (unordered) pairs (a, b) for which, over \mathbb{Q}_2 , the quaternion algebra $H_{a,b}$ does not split: it is those (a, b) for which $a \notin N(b)$ (and, of course, we need only consider a and b modulo squares). The next table lists those pairs and shows that, in each case,

$$4 + 8\mathbb{Z}_2 \subseteq S_{a,b}(\mathbb{Q}_2)$$

by assuming that we are given any $x_1 \equiv_2 2 \pmod{8}$ or $x_1 \equiv_2 6 \pmod{8}$ (which is equivalent to $2x_1 \equiv_2 4 \pmod{8}$) and by specifying elements x_2, x_3 and x_4 which guarantee that

$$-ax_2^2 - bx_3^2 + abx_4^2 \equiv_2 1 - x_1^2 \equiv_2 -3 \pmod{8}.$$

Multiplying x_2^2, x_3^2, x_4^2 by a suitable common element from $1 + 8\mathbb{Z}_2 \subseteq (\mathbb{Q}_2^\times)^2$,

makes then sure that $2x_1 \in S_{a,b}(\mathbb{Q}_2)$.

(a, b)	x_2	x_3	x_4
(2, 3)	0	1	0
(2, 5)	2	1	1
(2, 6)	0	1	$\frac{1}{2}$
(2, 10)	2	0	$\frac{1}{2}$
(3, 3)	1	0	0
(3, 10)	1	0	0
(3, 15)	1	0	0
(5, 6)	1	1	0
(5, 10)	1	0	1
(5, 30)	1	1	0
(6, 6)	$\frac{1}{2}$	$\frac{1}{2}$	0
(6, 15)	1	1	0
(10, 30)	0	1	$\frac{1}{10}$
(15, 15)	1	0	$\frac{2}{15}$
(15, 30)	1	1	$\frac{1}{15}$
(30, 30)	1	1	$\frac{1}{30}$

References

- [CSS] Jean-Louis Colliot-Thélène, Jean-Jacques Sansuc, Peter Swinnerton-Dyer, *Interactions of two quadrics and Châtelet surfaces I* resp. *II*, J. Reine Angew. Math. **373** (1987), 37-107 resp. **374** (1987), 72-168.
- [CZ] Gunther Cornelissen, Karim Zahidi, *Elliptic divisibility sequences and undecidable problems about rational points*, J. Reine Angew. Math. **613** (2007), 1-33.
- [F] Gerd Faltings, *Diophantine approximation on abelian varieties*, Annals of Mathematics **133** (1991), 549-576.
- [HS] Marc Hindry, Joseph H. Silverman, *Diophantine geometry*, Springer Graduate Texts in Mathematics 201, 2000.
- [K] Jochen Koenigsmann, *From p -rigid elements to valuations (with a Galois-characterization of p -adic fields)*, J. Reine Angew. Math. **465** (1995), 165-182.
- [P1] Bjorn Poonen, *Characterizing integers among rational numbers with a universal-existential formula*, Amer. J. Math. **131(3)** (2009), 675-682.

- [P2] Bjorn Poonen, *The set of nonsquares in a number field is diophantine*, Math. Res. Lett. **16(1)** (2009), 165-170.
- [R] Julia Robinson, *Definability and decision problems in arithmetic*, J. Symbolic Logic **14(2)** (1949), 98-114.
- [Sh] Alexandra Shlapentokh, *Using indices of points on an elliptic curve to construct a diophantine model of \mathbb{Z} and define \mathbb{Z} using one universal quantifier in very large subrings of number fields, including \mathbb{Q}* , arXiv:0901.4168v1 [math.NT], 27 Jan 2009.
- [Si] Joseph H. Silverman, *Integral points on abelian varieties*, Invent. math. **81** (1985), 341-346.

Mathematical Institute, 24-29 St Giles', Oxford OX1 3LB, UK
 koenigsmann@maths.ox.ac.uk